CERT-EU Security Advisory 2018-016

Signature Spoofing Vulnerability in GnuPG

June 15, 2018 — v1.0

History:

- *15/06/2018 — v1.0: Initial publication*

Summary

On 13th of June 2018, Marcus Brinkmann released technical details concerning a vulnerability impacting GnuPG and most applications based on GnuPG (Enigmail, GPGtools, python-gnupg, etc.) [1]. This vulnerability can be exploited by a remote attacker to spoof signatures in encrypted messages. Security researchers named those vulnerabilities **SigSpoof**.

To exploit the vulnerabilities, the `verbose` option needs to be enabled (via configuration file or via command line parameter). A successful exploitation of the vulnerability allows the attacker to spoof signature verification and message decryption results. Concerning Enigmail, exploitation of the vulnerability does not even need the message to be encrypted (encryption is spoofed as well).

Technical Details

The **SigSpoof** vulnerability exploits two design choices in GnuPG:

- some applications call GnuPG with `--status-fd 2` which combined `stderr` and the status messages in a single data pipe. The applications will then use line prefixes to parse the data pipe,
- GnuPG, with `verbose` enabled, does not escape newline characters when printing the name of the encrypted file to `stderr`.

By combining these flaws, the attacker can inject arbitrary (fake) GnuPG status messages into the application parser to spoof signature verification and message decryption results. The attacker can control the key IDs, algorithm specifiers, creation times and user IDs, and does not need any of the private or public keys involved.

A CVEs were provided for the vulnerability:

- CVE-2018-12020 [2]

Products Affected

Known affected products are:

- GnuPG before 2.2.8 and GnuPG before 1.4.23
- Enigmail before 2.0.7
- GPGTools before 2018.3

Other applications relying on GnuPG may also be affected.

Recommendations

- Upgrade to GnuPG 2.2.8 or GnuPG 1.4.23
- Upgrade to Enigmail 2.0.7
- Upgrade to GPGTools 2018.3

Workarounds

Is is highly recommended to disable `verbose` options to all invocations of GPG.

References

[1] https://neopg.io/blog/gpg-signature-spoof/#proof-of-concept-ii-signature-and-encryption-spoof-enigmail

[2] https://www.cvedetails.com/cve/CVE-2018-12020